AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: THOMAS SNYDER

Digitally signed by THOMAS SNYDER
Date: 2020.07.30 12:45:48 -05'00'

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

FILED

JUL 30 2020

CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY _____, DEPUTY

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF (1) A BLACK LG CELLULAR PHONE WITH IMEI 359962109901387 AND (2) A BLACK ANDROID CELLULAR PHONE, MODEL LT25H426271B CURRENTLY LOCATED IN SECURE EVIDENCE STORAGE AT THE OKLAHOMA CITY POLICE DEPARTMENT PROPERTY ROOM.

Case No. M-20-359-SM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession of Methamphetamine With Intent to Distribute

The application is based on these facts:

See attached Affidavit of Special Agent, Cristina Busbee, Homeland Security Investigations (HSI), which is incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cristina Busbee
Applicant's signature

Special Agent, Cristina Busbee (HSI)
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/30/20

Judge's signature

City and state: Oklahoma City, Oklahoma

Suzanne Mitchell, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF (1) A BLACK LG CELLULAR PHONE WITH IMEI 359962109901387 AND (2) A BLACK ANDROID CELLULAR PHONE, MODEL LT25H426271B CURRENTLY LOCATED IN SECURE EVIDENCE STORAGE AT THE OKLAHOMA CITY POLICE DEPARTMENT PROPERTY ROOM.	Case No. M-20-359-SM

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Cristina Busbee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices, as further described in Attachment A hereto—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since April 2019. I am presently assigned to the HSI office in Oklahoma City, Oklahoma (hereinafter referred to as HSI Oklahoma City).

3. I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am

authorized to conduct criminal investigations of violations of the laws of the United States and to execute warrants issued under the authority of the United States.

4. I have been involved in a wide variety of investigative matters. Among other things, I am responsible for conducting investigations into violations of federal criminal laws, including the smuggling of goods into the United States, aiding in unlawful importation, and the unlawful possession of firearms. I have received approximately 24 weeks of specialized training at the Federal Law Enforcement Training Center in the enforcement of federal laws. I have arrested, interviewed, and debriefed numerous individuals who have been involved with and have personal knowledge of smuggling goods into the United States, aiding in unlawful importation, and the unlawful possession of firearms, as well as, the amassing, spending, converting, transporting, distributing, laundering and concealing of proceeds from criminal activity. I have testified in judicial proceedings concerning the prosecution for violations of laws related to the smuggling of contraband and bulk cash. I have been the affiant of numerous federal search warrants. I have used these warrants to further criminal investigations.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched is (1) a black LG cellular phone with IMEI 359962109901387 and (2) a black Android cellular phone, model LT25H426271B, hereinafter

the "Devices", as further described in Attachment A hereto. The Devices are currently located in secure evidence storage at the Oklahoma City Police Department, 700 Colcord Drive, Oklahoma City, OK 73102.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. The Devices were seized from David SLONAKER (SLONAKER). As described in more detail below, SLONAKER is currently under investigation by HSI for violations of 21 U.S.C. § 841 (possession of methamphetamine with intent to distribute).

9. On June 10, 2020, at approximately 1900 hours, Oklahoma City Police Department (OCPD) officers conducted a traffic stop of a silver Ford Fiesta with a paper tag that was headed southbound on N. MacArthur Blvd. in Oklahoma City, OK. Officers had been conducting surveillance in the area of SLONAKER's suspected residence, an apartment at 5800 NW 34th St., Apt 14, Oklahoma City, OK. Officers observed SLONAKER leave apartment number 14 and get into the aforementioned vehicle. SLONAKER was the driver and sole occupant of the vehicle. Officers confirmed that SLONAKER had an outstanding and valid felony warrant out of Oklahoma County. Based on the warrant, officers conducted a traffic stop of SLONAKER's vehicle and he was arrested on the outstanding warrant.

10. During an inventory of the vehicle prior to it being impounded, officers located approximately 17 grams of methamphetamine and a Ruger .22 caliber pistol bearing serial number 22217189. Officers also located a digital scale and the two Devices. During a search of

SLONAKER's person, officers also discovered $5,216.00 in U.S. currency. Based on these findings, officers applied for a search warrant of SLONAKER's residence, 5800 NW 34th St., Apt 14, Oklahoma City, OK.

11. The search warrant, which was executed by OCPD officers and HSI agents at approximately 2100 hours on the same evening, resulted in the discovery of approximately 2.2 pounds of methamphetamine inside a safe, for which SLONAKER had a key. Officers also located a .22 caliber Ruger magazine, consistent with the pistol found in the vehicle when SLONAKER was arrested.

12. Based on the aforementioned facts, there is probable cause to believe that SLONAKER committed violations of 21 U.S.C. § 841 (possession of methamphetamine with intent to distribute). The Devices are currently located in secure evidence storage at the Oklahoma City Police Department, 700 Colcord Drive, Oklahoma City, OK 73102. In my training and experience, I know that the Devices have been stored in a manner in which their contents are (to the extent material to this investigation) in substantially the same state as they were when the Devices first came into the possession of investigators.

13. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

14. From my training and experience, I know that possession of narcotics with the intent to distribute are conspiratorially crimes. Individuals who engage in these crimes typically do so in groups with the assistance of others. These criminals often use their cell phones to communicate with other members of the transnational criminal organization. Records of these communications and the contact information of the smugglers are often saved in the individual's phone.

15. An examination can reveal the approximate location of the Device and the user by associating a specific date and time with: historical GPS data, historical cell-site data, and logs of Wi-Fi networks. Additionally, an examination can reveal the Device's unique identifiers (phone number, IMEI, IMSI, etc.). These unique identifiers can be used to compel material records from the cell phone service provider such as call logs, billing information, and historical cell-site data.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Cristina Busbee

Cristina Busbee
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on July 30, 2020:

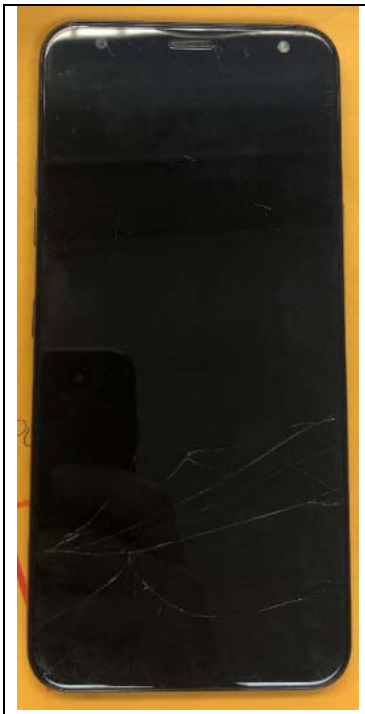
HON. SUZANNE MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

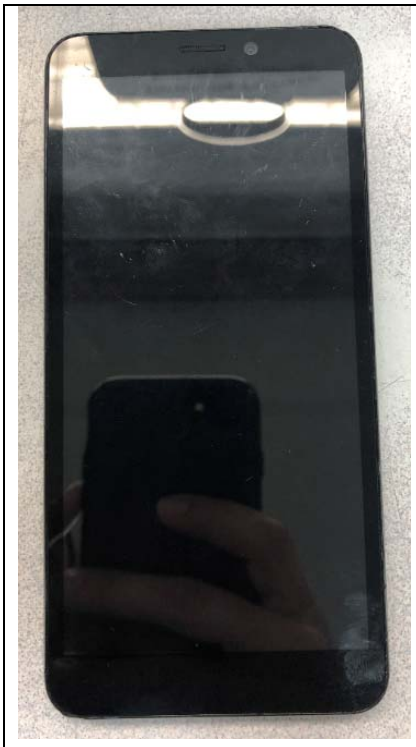
The properties to be searched are (1) a Black LG Cellular Phone with IMEI 359962109901387 and (2) a black Android cellular phone, model LT25H426271B, hereinafter the "Devices". The Devices are currently located in secure evidence storage at the Oklahoma City Police Department's property room.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

Black LG Cellular Phone with IMEI 359962109901387



Black Android Cellular Phone with Model Number LT25H426271B

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. § 841 involving David SLONAKER, including:

a. lists of customers and related identifying information;

b. types, amounts, and prices of drugs smuggled as well as dates, places, and amounts of specific transactions;

c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

d. any information recording David SLONAKER's schedule or travel;

e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.